InDret
REVISTA PARA EL
ANÁLISIS DEL DERECHO

WWW. INDRET.COM

Derecho al honor *online* y responsabilidad civil de ISPs

El requisito del "conocimiento efectivo" en las SSTS, Sala Primera, de 9 de diciembre de 2009 y 18 de mayo de 2010

Antoni Rubí Puig
Facultat de Dret
Universitat Pompeu Fabra

BARCELONA, OCTUBRE 2010

Abstract

*En supuestos de intromisiones al derecho al honor en la red, el "conocimiento efectivo" por parte de un prestador de servicios de la sociedad de la información (ISP) de la ilicitud del contenido alojado constituye el elemento principal que fundamenta la responsabilidad civil de aquél. Recientemente, la Sala Primera del Tribunal Supremo ha dictado dos sentencias, en 9 de diciembre de 2009 (asunto "*putasgae*") y 18 de mayo de 2010 (asunto "*quejasonline*"), en las cuales ha resuelto que es posible la acreditación de dicho elemento a partir de la comunicación efectuada por un afectado u otros datos que posibiliten su prueba* ex re ipsa.

El Tribunal, sin embargo, -al no requerirlo los casos de los que tuvo conocimiento- no ha examinado los límites a tales mecanismos de acreditación del "conocimiento efectivo". Este artículo traza algunos de los límites a la concreción del conocimiento efectivo y, en particular, señala la necesidad de que quien vea lesionado su derecho al honor tenga la carga primaria de desplegar cierto grado de diligencia para identificar razonablemente el contenido difamatorio y su carácter ilícito. La delimitación de deberes de cuidado entre ISP y perjudicado reduce los riesgos que un sistema de responsabilidad civil absoluta tiene sobre la innovación tecnológica y el funcionamiento y arquitectura de Internet.

*"Actual knowledge" of the illegal or tortious information stored by an Information Service Provider (ISP) stands as the main element to establish liability for online defamations. The Spanish Supreme Court has recently delivered two decisions –December 9Pth 2009 ("*putasgae*") and May 18th 2010 ("*quejasonline*")- in which has analyzed this element and held that it can be proved by means of a victim's notification or on* res ipsa loquitur *grounds.*

However, the Court, as the cases brought before it did not require so, missed the opportunity to discuss the limits to the aforementioned mechanisms in proving "actual knowledge". This article draws some of these limits and argues that victims of online defamations have a primary duty of care in reasonably identifying the presumably illegal or tortious information stored by the ISP. Establishing duties of care of both ISPs and victims reduces the risks that an absolute liability system would cast upon technological innovation and Internet's architecture.

Title: "Holding ISPs Liable for Online Defamations. The Element of «Actual Knowledge» in the Spanish Supreme Court Decisions of December 9th 2009 and May 18th 2010"

Palabras clave: Derecho al honor online, responsabilidad civil, ISPs, conocimiento efectivo
Keywords: Online Defamation, Civil Liability, ISPs, Actual Knowledge

Sumario

1. Conocimiento efectivo como criterio de imputación de daños

Facebook aloja más de 500 millones de perfiles de usuarios activos[1]. Google Search rastrea millones de páginas, cuyas direcciones puede enlazar después de que un usuario opere una búsqueda[2]. Cada minuto YouTube añade 24 nuevas horas de video a sus contenidos[3]. Con toda seguridad, parte de estos contenidos y de muchos de los alojados en la red infringe derechos de terceros o vulnera alguna norma legal de forma más o menos crasa: tanto los responsables de los prestadores de servicios de la sociedad de la información (en adelante, ISPs) como sus usuarios sabemos efectivamente que algunos de los contenidos disponibles en la red son injuriosos, que algunos otros vulneran derechos de propiedad intelectual, que otros suponen una intromisión en la intimidad ajena, que otros justifican el Holocausto o, incluso, que otros muestran imágenes de pornografía infantil. Lo saben. Lo sabemos.

También sabemos que las decisiones públicas sobre imputación de responsabilidad civil, penal y administrativa derivada de tales ilícitos instauran un juego de incentivos que condiciona la innovación tecnológica, así como el funcionamiento y la arquitectura de Internet. Atribuir responsabilidad civil absoluta a Google por daños causados por cualquier enlace a contenidos ilícitos eliminaría el carácter automático de las búsquedas y reduciría el catálogo de websites rastreado –sólo aquellos sitios que hubieran sido filtrados, seguramente después de haber pagado el precio que internalizara su responsabilidad potencial o de haber prometido un reembolso de gastos a Google Inc., serían objeto de un rastreo por el algoritmo desarrollado por Larry Page y Sergey Brin[4]-. Con una norma tal, la rapidez y eficacia que han caracterizado al buscador serían punto menos que imposibles[5].

---

[1] Mark ZUCKERBERG, "500 Million Stories", *Facebook Blog*, 21.7.2001 (http://blog.facebook.com/blog.php?post=409753352130) (Consultado en 24.9.2010).

[2] Según Jesse ALPERT y Nissan HAJAJ, ingenieros de Google, Inc., en 2008 el buscador llegó a contabilizar 1 billón de páginas web con URL únicas. Jesse ALPERT y Nissan HAJAJ, "We Knew the Web Was Big…", *The Official Google Blog*, 25.7.2008 (http://googleblog.blogspot.com/2008/07/we-knew-web-was-big.html) (Consultado en 24.9.2010).

[3] http://www.youtube.com/t/fact_sheet (Consultado en 24.9.2010).

[4] Ronald J. MANN y Seth R. BELZLEY, "The Promise of Internet Intermediary Liability", 47 *Wm. & Mary L. Rev.* 239 (2005).

[5] Véanse Mark A. LEMLEY, "Rationalizing Internet Safe Harbors", 6 *J. on Telecomm.& High Tech. L.* 101 (2007); y Frank PASQUALE, "Copyright in an Era of Information Overload: Toward the Privileging of Categorizers", 60 *Vand. L. Rev.* 133 (2007).

Los ordenamientos jurídicos, con una atención mayor o menor a los incentivos que generan las decisiones normativas, han incorporado normas que sirven para delimitar la responsabilidad por hecho ajeno en que pueden incurrir los ISPs por datos o contenidos creados por sus usuarios, que desplazan en unos casos o complementan en otros las reglas sobre responsabilidad vicaria o *Respondeat Superior*.

Las dos normas más importantes son, en la Unión Europea, la *Directiva 2000/31/CE, del Parlamento Europeo y del Consejo, de 8 de junio, relativa a determinados aspectos de los servicios de la sociedad de la información, en particular, el comercio electrónico en el mercado interior* [6] –así como las diferentes normas de transposición a los derechos nacionales-; y, en Estados Unidos, el artículo 230 de la *Communications Decency Act* (CDA)[7].

Excede del objeto de este trabajo el examen de la superioridad de una u otra norma en relación con sus efectos sobre la innovación técnica y el bienestar social. Solamente cabe apuntar que la responsabilidad civil potencial de los ISPs es mucho mayor en la normativa europea que en la norteamericana. En particular, en los supuestos de intromisiones al derecho al honor –objeto de este trabajo-, el artículo 230 CDA blinda a los ISPs frente a cualquier pretensión de responsabilidad civil ejercida por la víctima de un libelo[8]:

> Sec. 230 (c)(1)
> *No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.*
>
> Sec. 230 (e)(3)

[6] DO L 178 de 17.7.2000, p. 1.

[7] 47. U.S.C. § 230.

[8] El artículo 230 de la *Communications Decency Act* ofrece un régimen de protección de los ISPs frente a posibles contingencias de responsabilidad civil derivadas de ilícitos civiles desarrollados en el *Common Law* (tales como los *torts* de *defamation*, *liberl, slander, disparagement, invasion of privacy*, *misrepresentation* o *negligence*) o desplegados por los derechos estatales (por ejemplo, el *right of publicity*, aunque varios tribunales consideran que no resulta de aplicación este régimen a la lesión de aquél) . Sin embargo, algunas lesiones de derechos –notablemente de derechos de autor y derechos de marcas- quedan fuera del ámbito de aplicación de la norma (47. U.S.C. § 230(e)) y resultan de aplicación otras normas federales –en el caso de derechos de autor, la Digital Millennium Copyright Act (DMCA), 17 U.S.C. §512, y en el de derechos marcarios, la Lanham Act, 15 U.S.C. § 1114 (2)(B)-(C). Véase, por todos, David S. ARDIA, "Free Speech Savior or Shield for Scoundrels: An Empirical Study of Intermediary Immunity Under Section 230 of the Communications Decency Act", 43 *Loyola of Los Angeles Law Review* 373 (2010).

Para un examen del régimen europeo y el norteamericano en el ámbito de la infracción de derechos de autor, véase Miquel PEGUERA POCH, "The DMCA Safe Harbors and Their European Counterparts: A Comparative Analysis of Some Common Problems", 32 *Colum. J. L. & Arts* 481 (2008-2009).

> *No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section.*

En cambio, la Directiva 2000/31/CE permite atribuir a ISPs responsabilidad civil por intromisiones al derecho al honor. En relación con los prestadores de servicios de alojamiento de datos, el artículo 14 establece:

> 1. Los Estados miembros garantizarán que, cuando se preste un servicio de la sociedad de la información consistente en almacenar datos facilitados por el destinatario del servicio, el prestador de servicios no pueda ser considerado responsable de los datos almacenados a petición del destinatario, a condición de que:
>
> a) el prestador de servicios no tenga conocimiento efectivo de que la actividad a la información es ilícita y, en lo que se refiere a una acción por daños y perjuicios, no tenga conocimiento de hechos o circunstancias por los que la actividad o la información revele su carácter ilícito, o de que,
>
> b) en cuanto tenga conocimiento de estos puntos, el prestador de servicios actúe con prontitud para retirar los datos o hacer que el acceso a ellos sea imposible.

En España, la *Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico*[9], que transpuso la Directiva 2000/31/CE a nuestro ordenamiento, establece, en su artículo 16, la concurrencia de los dos mismos requisitos –conocimiento efectivo de la ilicitud e incumplimiento de deber de retirada- para atribuir responsabilidad civil a un proveedor de servicios de alojamiento de datos[10]:

> 1. Los prestadores de un servicio de intermediación consistente en albergar datos proporcionados por el destinatario de este servicio no serán responsables por la información almacenada a petición del destinatario, siempre que:

[9] BOE núm. 166, de 12.7.2002.

[10] Véanse José Manuel BUSTO LAGO, "La responsabilidad civil de los prestadores de servicios de la sociedad de la información (ISPs)", en Luis Fernando REGLERO (Ed.), *Tratado de Responsabilidad Civil*, Tomo II, 4ª ed., Thomoson-Aranzadi, Cizur Menor, 2008; y Maria Magdalena PAYERAS CAPELLÀ y Santiago CAVANILLAS MÚGICA, "Los servicios de acceso y alojamiento: descripción técnica y legal", en Santiago CAVANILLAS MÚGICA, *Deberes y responsabilidades de los servidores de acceso y alojamiento. Un análisis multidisciplinar*, Comares, Granada, 2005.

> a) No tengan conocimiento efectivo de que la actividad o la información almacenada es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o
>
> b) Si lo tienen, actúen con diligencia para retirar los datos o hacer imposible el acceso a ellos.
>
> Se entenderá que el prestador de servicios tiene el conocimiento efectivo a que se refiere el párrafo a) cuando un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse.

El conocimiento efectivo por parte del ISP de la ilicitud del contenido alojado constituye, sin duda, el elemento principal que fundamenta la responsabilidad civil de aquél. Sin embargo, no se trata de un elemento que pueda concretarse de forma automática por un juez y la jurisprudencia menor no ha sido uniforme en su identificación[11].

El artículo 16.1.2 de la Ley 34/2002 prevé algunas pautas de concreción pero no restringe la posibilidad de nuevos medios para determinar la existencia de conocimiento efectivo[12]:

a) Conocimiento de una resolución judicial o administrativa que declare la existencia de una lesión o de la ilicitud de los contenidos.

b) Conocimiento a partir de los procedimientos de detección y retirada de contenidos adoptados voluntariamente por un ISP.

c) "Otros medios de conocimiento efectivo que pudieran establecerse".

La ductilidad de un requisito como el de "conocimiento efectivo" abruma. Por una parte, "conocimiento efectivo" excluye más de lo deseable: al presuponer la posibilidad de conocimiento por parte de un ISP, calidad predicable sólo de individuos, la norma exoneraría de responder a los ISPs organizados societariamente. Por otra parte,

[11] Miquel PEGUERA POCH, "«Sólo sé que no sé nada (efectivamente)»: la apreciación del conocimiento efectivo y otros problemas en la aplicación judicial de la LSSI", *IDP Revista d'Internet, Dret i Política* número 5 (2007), págs. 2-18 (disponible en http://www.uoc.edu/idp/5/dt/esp/peguera.pdf), p. 11.

[12] José Manuel BUSTO LAGO, *op. cit.*, pp. 1038-1045.

"conocimiento efectivo" incluye también más de lo deseable: hemos empezado este artículo afirmado que todos conocemos efectivamente que la probabilidad de que la red almacene contenidos ilícitos es 1.

La primera desnaturalización de la norma encuentra su solución en la aplicación de las reglas de responsabilidad civil por hecho ajeno (artículo 1903.4 CC) que atribuyen al principal, el ISP, las consecuencias económicas derivadas de lo que efectivamente conocen sus dependientes. La solución a la segunda desnaturalización –que constituye el objeto de este artículo- pasa por la necesaria delimitación de deberes de cuidado, tanto del ISP como del perjudicado, en relación con un contenido ilícito determinado, para evitar la creación judicial de un sistema de responsabilidad civil absoluta.

Recientemente el Tribunal Supremo ha dictado dos sentencias en las que se ha pronunciado sobre la responsabilidad de ISPs por intromisiones al derecho al honor, que sirven para identificar el alcance del requisito del "conocimiento efectivo". Sin embargo, las particularidades de ambos casos han hecho innecesaria la consideración de los límites a la imputación de responsabilidad mediante la delimitación de deberes de cuidado de uno y otro litigante.

2. Conocimiento efectivo en la jurisprudencia del Tribunal Supremo

2.1. STS, 1ª, de 9.12.2009 (RJ 2010, 131; MP: José Ramón Ferrándiz Gabriel). *SGAE y Teddy Bautista c. Asociación de Internautas.*

A principios de los 2000, un grupo de internautas elaboró una página web crítica con las maneras usadas por la Sociedad General de Autores y Editores (SGAE) en defensa de los derechos de sus asociados. La crítica quedaba, sin embargo, mediatizada por el insulto: los autores de los contenidos se autodenominaban "Realmente Cabreados con la SGAE", el nombre de dominio que registraron para difundirlos fue www.putasgae.com, y en tal dirección se incluyeron expresiones en las que calificaban a la SGAE como "una banda de desocupados", "ladrones", "oportunistas sanguijuelas", "autores de redadas fascistoides", "matones a sueldo", "pandillas de mafiosos" o "putos chorizos", entre otros.

La SGAE presento entonces una demanda para la cancelación del citado nombre de dominio ante el Centro de Arbitraje y Mediación de la OMPI, que fue estimada por Decisión de 18 de diciembre de 2002 (Caso No. D2002-0953). El Centro resolvió la existencia de un riesgo de confusión entre el nombre de dominio y las marcas titularidad de SGAE, así como un uso de mala fe por parte de los demandados. En particular, el Centro concluyó que la afrenta al honor de la SGAE era más que clara: "el uso de la palabra "puta" delante del vocablo "sgae" se hace con un claro sentido denigratorio y agresivo hacia una persona jurídica (la de la

Demandante) y hacia la actividad por ella desarrollada. No puede haber justificación en el uso de un término tan peyorativo, mal sonante, denigratorio y abyecto como el anteriormente citado, y menos aún cuando tal uso se hace en un contexto en el que claramente se pretende ridiculizar la actividad desarrollada por la Demandante o por sus integrantes, como se puede comprobar con solo visitar la página web correspondiente, […E]l Demandado no puede amparar su conducta en el ejercicio de los derechos fundamentales de libertad de expresión y en el derecho a recibir información".

Ante la cancelación del dominio www.putasgae.com, la Asociación de Internautas alojó, bajo el subdominio hhtp://antisgae.internautas.org, un *mirror* del website en su propio sitio web y anunció públicamente su acción. Textualmente señaló: "Desde este momento la Asociación de Internautas ofrece cobertura organizativa, legal y de difusión entre sus socios y simpatizantes en su sitio web a esta plataforma"[13].

La SGAE y el presidente de su consejo de dirección, Eduardo (Teddy) BAUTISTA GARCÍA, demandaron a la Asociación de Internautas por intromisión en el derecho al honor y solicitaron el cese de los insultos y una indemnización de 18.000 euros para cada uno de los actores.

El JPI num. 42 de Madrid en sentencia de 15.6.2005 estimó la demanda. Interpuesto recurso por la demandada, la AP de Madrid, Sección 19ª, confirmó en sentencia de 6.2.2006 (AC 2006, 188) la dictada por el Juzgado.

La Asociación de Internautas interpuso recurso de casación denunciando la infracción de los artículos 18 y 20 de la Constitución y el artículo 16 de la Ley 34/2002. Para la recurrente, el concepto de "conocimiento efectivo" debía entenderse restrictivamente y alcanzar solamente aquellos supuestos en los cuales un ISP hubiera conocido una resolución que declarara la ilicitud de los contenidos, ordenara su retirada, imposibilitara el acceso a los mismos o resolviera la existencia de una lesión.

Una interpretación tal, para el Tribunal, "reduce injustificadamente las posibilidades de obtención del "conocimiento efectivo" de la ilicitud de los contenidos almacenados y amplía correlativamente el ámbito de la exención" (FD 4º).

El Tribunal Supremo resuelve que un conjunto de circunstancias pueden servir para acreditar la existencia de conocimiento efectivo (*res ipsa loquitur*) y, así, evita entrar en la discusión de si la Decisión del Centro de Arbitraje y Mediación de la OMPI podría constituir una resolución de un "órgano competente", con arreglo al artículo 16.1 de la Ley 34/2002. El Tribunal hace suyas las palabras de la Audiencia Provincial, según la cual el conocimiento

[13] http://www.internautas.org/html/836.html (Consultado en 24.9.2010).

efectivo puede obtenerse "*a partir de hechos o circunstancias aptos para posibilitar, aunque mediatamente o por inferencias lógicas al alcance de cualquiera, una efectiva aprehensión de la realidad de que se trate*" (FD 4º).

En este sentido, para el Tribunal, el conocimiento efectivo era evidente: "*tal título [putasgae], por su carácter insultante, era un medio adecuado –ex re ipsa- para revelar, junto con las circunstancias concurrentes –en especial, la realidad de un conflicto entre dicha proveedora de contenidos y la entidad de gestión de derechos de propiedad intelectual demandante, conocido por la recurrente-, el tenor injurioso de los datos alojados*" (FD 4º).

2.2. STS, 1ª, de 18.5.2010 (RJ 2010, 2319; MP: José Ramón Ferrándiz Gabriel). Luis Alberto c. Ruboskizo, S.L.

www.quejasonline.com consiste en una plataforma titularidad de la mercantil Ruboskizo, S.L. en la cual sus usuarios pueden redactar y publicar notas de queja sobre productos adquiridos o servicios prestados por terceros. Si bien los usuarios del sitio web deben indicar su nombre y su dirección de correo electrónico para publicar una queja, es posible hacerlo proporcionando datos falsos o ajenos.

El día 4 de junio de 2004, www.quejasonline.com publicó una nota, cuya autoría se atribuía a Luis Alberto, con el texto siguiente: "Soy abogado de la Mutua Madrileña y estoy cansado de engañar a la gente, pues la Mutua me hace retrasar los expedientes con el fin de no pagar, tiene pinta de irse al garete".

Luis Alberto, abogado en ejercicio en Valencia desde 1975 y cuyo cliente principal era la «Mutua Madrileña Automovilística», informó a Ruboskizo, S.L. de la utilización falsa de su nombre y solicitó la retirada de la queja de www.quejasonline.com, así como la identidad del remitente. Ruboskizo S.L. retiró la nota de queja y le indicó que no podía identificar al autor del contenido.

Después de que Luis Alberto iniciara un proceso penal, cuyas actuaciones fueron archivadas por el desconocimiento del autor de los hechos, demandó a Ruboskizo, S.L. y solicitó una indemnización de 6.135,17 euros por los daños y perjuicios a su honor.

El Juzgado de Primera Instancia núm. 23 de Valencia, en sentencia de 30.11.2006, estimó la demanda. La Audiencia Provincial de Valencia, Sección 6ª, desestimó el recurso de apelación de la demanda y confirmó la sentencia de instancia.

El Tribunal Supremo, en sentencia de 18 de mayo de 2010, declaró haber lugar al recurso de casación interpuesto por la demandada, casó la sentencia de la Audiencia y desestimó la demanda interpuesta por Luis Alberto. Para el Tribunal Supremo, la Audiencia Provincial no

aplicó el artículo 16 de la Ley 34/2002 para la fundamentación de la posible responsabilidad de Ruboskizo, S.L., como prestador de servicios de alojamiento de datos y, por ello, "no ha extraído consecuencia alguna de que dicha sociedad no conociera ni pudiera razonablemente conocer, directamente o a partir de datos aptos para posibilitar la aprehensión de la realidad, que quien le suministraba el contenido lesivo para el demandante no era él, sino otra persona que utilizaba indebidamente su nombre con el ánimo de perjudicarle, ni de que, conocedora con posterioridad de esa realidad, merced al requerimiento del perjudicado, retirase el comentario sin tacha de negligencia" (FD 2º).

Esto es, los responsables de www.quejasonline.com conocieron, no en el momento de que los contenidos se publicaron en el sitio web sino a partir de la comunicación efectuada por el demandante[14], el carácter lesivo del contenido publicado y, al retirarlo de la página web, cumplieron con el deber de diligencia que exige el artículo 16.1 b) de la Ley 34/2002.

Así pues, para el Tribunal Supremo, la mera comunicación por el perjudicado –desconocemos la forma y el contenido de la comunicación, así como su grado de sofisticación- es suficiente para determinar la existencia de un "conocimiento efectivo" por parte del ISP. En efecto, el Tribunal Supremo hace referencia a la obtención de conocimiento "directamente o a partir de datos aptos para posibilitar la aprehensión de la realidad".

El hecho de que los responsables de www.quejasonline.com retiraran el contenido identificado impide anticipar una respuesta del Tribunal para el supuesto en que el ISP hubiera mantenido el contenido en la red. No es posible predecir cuál hubiera sido la respuesta del Tribunal Supremo y si hubiera establecido algún tipo de límites a la comunicación realizada por un afectado como mecanismo de acreditación del conocimiento efectivo.

3. La necesaria delimitación de deberes de cuidado en la identificación del conocimiento efectivo

[14] La distinción que el Tribunal hace en el FD 4º de la sentencia entre "conocimiento" en el momento de alojamiento de los datos y "conocimiento" de su ilicitud con posterioridad es innecesaria. El artículo 16 de la Ley 34/2002 no establece ningún punto de conexión temporal para la determinación del consentimiento efectivo. De hacerlo, convertiría en inoperable a la norma en la mayoría de casos, dado el carácter continuado de la prestación de servicios de alojamiento. Sin embargo, véase Antònia PANIZA FULLANA, "El alcance de la responsabilidad de los prestadores de servicios de la sociedad de la información", *Aranzadi Civil*, núm. 4/2010, afirmando que, en la sentencia aquí comentada, el Tribunal Supremo "*considera que la sociedad demandada titular de la página web en la que se ha vertido el comentario objeto de litigio no conocía ni podía razonablemente conocer ni directa ni indirectamente el contenido lesivo ya que no podía saber que quien había escrito el comentario no era realmente quien decía ser*".

3.1. Insuficiencia de un criterio restrictivo fundado en la decisión previa de un órgano competente

En las sentencias citadas, la acreditación del conocimiento efectivo no queda limitada a la existencia de una decisión de un órgano competente que hubiera "declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión". Para la Sala Primera del Tribunal Supremo, es dable probar el conocimiento efectivo "*a partir de datos aptos para posibilitar la aprehensión de la realidad*" y, en algunas circunstancias, tales datos permitirán incluso presumir el conocimiento de la ilicitud del contenido *ex re ipsa*.

De entrada, la solución adoptada por el Tribunal se ajusta a la literalidad de la Ley 34/2002, cuyo artículo 16.1 refiere la posibilidad de recurrir a "otros medios de conocimiento efectivo que pudieran establecerse". La solución también se ajusta a la Directiva 2000/31, que no especifica formas de concreción del "conocimiento efectivo" por parte de un ISP y permite su delimitación a los Estados Miembros.

La solución es plausible en supuestos en los cuales la intromisión en el derecho al honor es manifiesta, como ocurría en el asunto "putasgae". El uso de la palabra "puta", así como otras expresiones injuriosas contenidas en el sitio web, revelaban un claro ánimo difamatorio que sobrepasaba los límites de la libertad de expresión. En casos en los cuales la intromisión es autoevidente, esperar a la existencia de una resolución administrativa o una decisión judicial firme agrava la posición del perjudicado, que ha de arrostrar con la persistencia de la difamación en la red hasta que la decisión gane firmeza y pueda ser comunicada al ISP que alberga los contenidos en cuestión. Esperar meses, o incluso años, para que el ISP esté obligado a retirar el contenido incrementa irrazonablemente los daños causados en supuestos de lesiones manifiestas del derecho al honor.

La necesidad de disponer de una decisión judicial o administrativa también agrava la posición del perjudicado si éste no puede identificar el autor del contenido contra el que dirigir su acción, ya porque resulte imposible dado el carácter anónimo de la prestación de los servicios o porque no exista una obligación privada del ISP de colaborar en la identificación del autor del contenido –escudado básicamente en la normativa sobre protección de datos personales-. Las dificultades de identificación de un sujeto contra el que dirigir una acción para obtener una decisión de un órgano competente cuestionan la bondad de un sistema de acreditación del conocimiento efectivo de la ilicitud basado en la declaración previa de un órgano competente. Pero, además, las dificultades en la identificación del causante de un daño constituyen una de las razones que abogan por el

establecimiento de un régimen de responsabilidad por hecho ajeno, como el previsto en el artículo 16 de la Ley 34/2002[15].

En efecto, resulta necesario tener en cuenta la posibilidad de otras formas de acreditar el conocimiento efectivo y ésta es la vía que ha abierto en el Tribunal Supremo en las dos sentencias comentadas en este artículo. En especial, resulta necesario examinar el alcance de las comunicaciones recibidas por un ISP de un tercero que alega haber sufrido una lesión en su derecho al honor, así como los límites a estos mecanismos, una cuestión no tratada por el Tribunal Supremo por no requerirlo los casos que llegaron a su conocimiento.

3.2. Delimitación de deberes de cuidado entre ISP y perjudicado

En la sentencia de 9 de diciembre de 2009, el Tribunal Supremo cita el Considerando 48 de la Directiva 2000/31, que establece que: "La presente Directiva no afecta a la posibilidad de que los Estados miembros exijan a los prestadores de servicios, que proporcionan alojamiento de datos suministrados por destinatarios de su servicio, que apliquen un deber de diligencia, que cabe esperar razonablemente de ellos y que esté especificado en el Derecho nacional, a fin de detectar y prevenir determinados tipos de actividades ilegales". La cita parece superflua, pues el considerando en cuestión se refiere a mecanismos preventivos o *ex ante* y no a la actuación *ex post* del ISP una vez el contenido ya está almacenado en sus equipos. Sin embargo, el considerando sirve al Tribunal Supremo para calificar tanto la obtención de conocimiento como la obligación de retirada posterior como deberes de cuidado:

> "Se condiciona la exclusión de responsabilidad al cumplimiento de un deber de diligencia para conocer la ilicitud –letra a)- e impedir su persistencia –letra b)" (FD 2º).

Recurrir a un juicio de diligencia permite considerar los límites de mecanismos de obtención de conocimiento efectivo por parte de un ISP alternativos a la comunicación de una decisión de un "órgano competente" y valorar la posible exoneración del ISP que ha tenido sólo un conocimiento fragmentario o indiciario del carácter ilícito de los datos alojados.

No cualquier tipo de comunicación por parte de un afectado debería obligar a actuar a un ISP, mediante la retirada de los contenidos presuntamente ilícitos que almacena o mediante una contestación al afectado: la decisión de un ISP de mantener el alojamiento de unos datos después de haber tenido conocimiento de su posible ilicitud puede calificarse de diligente si la comunicación recibida del afectado no reviste cierto grado de razonabilidad, salvo que

[15] Alan O. SYKES, "The Economics of Vicarious Liability", 93 *Yale Law Journal* 1231 (1984); Alan O. SYKES, "The Boundaries of Vicarious Liability: An Economic Analysis of the Scope of Employment Rule and Related Legal Doctrines", 101 *Harvard Law Review* 563 (1988); y Pablo SALVADOR CODERCH et al., "Respondeat Superior I", *InDret* 2/2002 (www.indret.com).

existan circunstancias adicionales que manifiesten la existencia de un conocimiento efectivo[16]. En otros términos, la diligencia debida por el ISP dependerá en buena medida de la diligencia desplegada por el perjudicado.

El conocimiento efectivo de la ilicitud de los contenidos alojados por un ISP debe responder a fuentes razonables: no debería bastar cualquier tipo de conocimiento indiciario o comunicación de un afectado. En particular, no debería bastar que un usuario de un contenido calificara el contenido como inapropiado o ilícito (por ejemplo, mediante sistemas de calificación ("*red flags*")), ni un simple correo electrónico señalando el malestar de un usuario con un determinado contenido. Así pues, si el perjudicado no actúa diligentemente en primer lugar, satisfaciendo un determinado grado de razonabilidad en su comunicación, no habría posibilidad de imputar responsabilidad al ISP, salvo que concurrieran circunstancias adicionales. La solución propuesta reproduciría el funcionamiento de una regla de negligencia contributiva.

A falta de la previsión de un sistema de notificación y retirada de contenidos ("*notice and take down*") en la Ley 34/2002, puede resultar deseable que los tribunales identifiquen deberes de cuidado y realicen juicios de imputación subjetiva para delimitar la responsabilidad civil de los ISPs en el ámbito de la difamación *online* o en otros ilícitos civiles. Tal tarea pasa principalmente por identificar el grado de razonabilidad de la comunicación efectuada por un afectado o, en otros términos, el grado de diligencia desplegado en su redacción y tramitación.

La necesidad de cierto grado de diligencia en la víctima se funda en las exigencias derivadas de la tutela de bienes e intereses propios que impone a su titular la carga primaria de su protección: quien alega una vulneración en su derecho al honor es quien está mejor situado para identificar su origen y, hasta cierto punto, su carácter ilícito.

Pero, además, atribuir responsabilidad sin contemplar el grado de diligencia del afectado puede comportar riesgos sustanciales para la libertad de expresión e información, dada la fragilidad del compromiso de los ISPs en relación con el contenido que albergan y facilitan. Los intereses de los prestadores de servicios y de sus usuarios divergen[17]: si se imponen

[16] Por ejemplo, en el caso "putasgae", una circunstancia adicional determinante de la responsabilidad *ex re ipsa* es el apoyo público que el alojador de los datos mostró a la campaña contra la SGAE. Tal apoyo y su decisión de permitir su inclusión en su website sitúan al ISP en una posición más próxima a la de editor que a la de almacenador de datos o, si se prefiere, más próxima al régimen de responsabilidad directa que al de responsabilidad por hecho ajeno.

[17] Jack M. BALKIN, "The Future of Free Expression in a Digital Age", 36 *Pepp. L. Rev.* 427 (2009). BALKIN señala que las editoriales y los periódicos tienen un interés en defender la expresión de los autores y periodistas que respectivamente publican, mientras que la falta de una relación de dependencia entre un ISP

todos los costes a los ISPs derivados de los contenidos creados por terceros, pero estos no pueden capturar todos los beneficios sociales de tales contenidos –como ocurre con la expresión y la información dado su carácter de bien público-, los ISPs van a reaccionar restringiendo de forma ineficiente los usos que terceras partes puedan hacer de Internet[18] y van a retirar más contenidos de los estrictamente ilícitos.

Exigir un mínimo de diligencia en la redacción de la comunicación de un afectado evita que parte de las reclamaciones más frívolas o de bagatela tengan lugar. Con todo, incluso con un sistema de notificación formal y retirada, el riesgo de reclamaciones injustificadas persiste: en el ámbito de los derechos de autor, algunos autores han señalado que un mínimo de un 30 % de las notificaciones recibidas por ISPs carece de fundamento jurídico[19]. A pesar de ello, dada la divergencia de intereses entre ISPs y sus usuarios, los primeros responden casi siempre eliminando el contenido identificado como ilícito por un usuario. Para el ISP, ello resulta más barato y sencillo que realizar un control de fondo de la ilicitud del contenido, que, además, difícilmente puede ser automatizado: por ejemplo, un software de filtrado difícilmente si una determinada expresión injuriosa en un contenido está justificada dado el carácter de reportaje neutral del texto o si su la información es veraz porque su autor agotó la diligencia exigible en contrastar los datos.

Cuando un ISP retira contenido potencialmente lesivo lo hace habitualmente sin ofrecer una oportunidad a su autor para oponerse a la retirada. Ofrecer tales sistemas de resolución de controversias entre usuarios es costoso para los ISPs y más oneroso que borrar el contenido directamente[20]. Sin embargo, la retirada de contenidos –por ejemplo la eliminación de todos los contenidos de un blog y de la cuenta de su usuario- ante una reclamación infundada podría generar responsabilidad contractual en el ISP[21].

---

y su usuario elimina los incentivos del ISP a defender los derechos de expresión de sus usuarios, pp. 435-436.

[18] Mark A. LEMLEY, *op. cit.*, p. 112.

[19] Jennifer M. URBAN y Laura QUILTER, "Efficient Process or "Chilling Effects"? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act", 22 *Santa Clara Computer & High Tech. L.J.* 621 (2006).

[20] Seth KREIMER, "Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link", 155 *U. Pa. L. Rev.* 11 (2006).

[21] Por supuesto, el alcance de tal responsabilidad dependerá del contrato suscrito entre ISP y usuario o de las condiciones de uso del servicio –con los límites del derecho de protección de consumidores, en su caso-. Dado el carácter gratuito de muchos servicios de almacenamiento de datos, es habitual la exclusión de la responsabilidad. Con todo, muchos ISPs establecen medidas de protección adicionales, tales como la supresión de una cuenta de usuario después de tres reclamaciones efectuadas por personas diferentes y en fechas diferentes o la conservación temporal de una copia de los datos eliminados.

3.3. Concreción de los deberes de cuidado del perjudicado

Discutida la conveniencia de que quien ve lesionado su derecho al honor –o, en su caso, otros derechos y bienes- tenga la carga primaria de desplegar cierto grado de diligencia para identificar razonablemente el contenido difamatorio y su ilicitud, resulta preciso señalar en qué puede consistir tal grado de diligencia.

Por supuesto, el grado de diligencia dependerá de las circunstancias particulares de cada caso, pero es posible establecer unos mínimos que ofrezcan una aproximación a un régimen de notificación deseable. El elemento principal que convierte a una comunicación de un afectado en razonable es la correcta identificación del contenido lesivo: por ejemplo, no resultan suficientes mensajes del tipo "todos los videos alojados en YouTube que muestran a mi persona" o "todos los videos alojados en YouTube que reproducen la rueda de prensa en la que el Sr. X lesionó mi honor al pronunciar las expresione a, b y c". Es precisa la identificación de URLs concretas, para que el ISP pueda fácilmente localizar el contenido y examinar su posible ilicitud.

En este sentido, uno de los regímenes que los tribunales pueden tener en cuenta a la hora de concretar los deberes de cuidado tanto del particular que ve lesionados sus derechos como del ISP es el previsto en la legislación norteamericana sobre responsabilidad de prestadores de servicios de alojamiento por infracciones de derechos de autor (§ 512(c) de la *Digital Millennium Copyright Act* (DMCA)[22]). Se trata de un sistema de notificación ya probado, con una trayectoria histórica de doce años, y, sobre todo, utilizado en España y en otros países

[22] 17 U.S.C. § 512(c)(3): "Elements of notification.— (A) To be effective under this subsection, a notification of claimed infringement must be a written communication provided to the designated agent of a service provider that includes substantially the following: (i) A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed. (ii) Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site. (iii) Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material. (iv) Information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted. (v) A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law. (vi) A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed".

por ISPs con sede principal en los EE.UU.[23], lo que lo convierte o lo sitúa próximo a los usos del comercio en este sector.

Así, en líneas generales, una comunicación por parte de quien considerara vulnerado su derecho al honor podría calificarse de diligente si constara por escrito y contuviera elementos como una firma o firma electrónica del perjudicado o de la persona autorizada a actuar en nombre de aquél y sus datos de contacto –especialmente, una dirección de correo electrónico-; la identificación completa de la persona cuyo honor se ha afectado; la identificación del contenido que se reputa difamatorio y cuya retirada se solicita, especialmente, mediante la indicación de URLs u otra forma de facilitar la contrastación del contenido por parte del ISP; y, acaso, una declaración de que el reclamante cree de buena fe que las manifestaciones realizadas en el contenido en cuestión son ilícitas y no están amparadas en la libertad de información y expresión. Por supuesto, no se trata de aplicar una norma propia de otro ordenamiento sino la utilización de sus pautas como elementos útiles para definir criterios de imputación de daños. Si se prefiere, se trata de importar a bajo coste tecnología jurídica desarrollada en otro país que, de hecho, muchos ISPs ya utilizan en el mercado español.

La necesidad de delimitar tales deberes de cuidado mediante una obligación de colaboración del perjudicado en la identificación de los contenidos ilícitos ha sido puesta de relieve, en el ámbito de la infracción de derechos de autor, por la Sentencia del Juzgado de lo Mercantil núm. 7 de Madrid de 20.9.2010 en el asunto *Telecinco c. YouTube* (MP: Andrés Sánchez Magro).

Las sociedades "Gestevisión Telecinco, S.A." y "Telecinco Cinema S.A.U" (en adelante, Telecinco) ejercitaron acciones por infracción de derechos de autor contra "YouTube LLC" al entender que la difusión mediante el sitio web propiedad de la demandada de grabaciones audiovisuales de Telecinco constituía una infracción de derechos de propiedad intelectual[24].

La Sentencia citada desestima la demanda, principalmente en aplicación del artículo 16.1 de la Ley 34/2002 sobre responsabilidad civil del prestador de servicios de alojamiento de datos. Frente a la alegación de la parte actora de que la acreditación del conocimiento

[23] El sistema previsto en la DMCA es el sistema de notificación que funciona a la práctica en nuestro país y que es implementado por aquellos ISPs más conocidos en el mercado. Véanse las siguientes páginas relativas a Facebook (http://www.facebook.com/legal/copyright.php?howto_report#!) ; YouTube: (Thttp://www.youtube.com/t/dmca_policy); y Google (http://www.google.com/dmca.html) (Consultadas en 24.9.2010).

[24] Véase, para unos hechos y sentencia muy similares, el asunto *Viacom y otros c. Youtube* resuelto por el Tribunal de Distrito del *Southern District* de Nueva York el pasado 23 de junio de 2010.

efectivo puede derivarse del conocimiento generalizado de que en el sitio web de la demandada se difunde contenido ilícito, el Magistrado ponente de la sentencia señala:

> "[…E]l conocimiento deberá acreditarse pormenorizadamente, no bastando la mera sospecha o el indicio racional para probarlo. Esa concretización del conocimiento efectivo exige sin duda la colaboración del perjudicado. […]
>
> Lo que esto significa en el caso concreto es que partiendo del principio general firmemente establecido de que la demandada no tiene obligación alguna de monitorizar o controlar con carácter previo los contenidos alojados en su Sitio web, corresponde a la actora poner en conocimiento efectivo de YouTube aquellos contenidos que puedan lesionar o infringir la titularidad de sus derechos de propiedad intelectual. Y debe hacerlo no de una forma masiva e incondicionada, sino individualizada y concreta […].
>
> [H]emos de convenir que no se trata de un procedimiento cómodo y sencillo para la actora, particularmente porque le incumbe la ingrata tarea de rastrear y controlar los contenidos que se alojan en la página web de la demandada. Pero ello responde justamente al orden de prioridades que tanto el legislador comunitario como el nacional han establecido".

4. Conclusiones

La identificación del "conocimiento efectivo" acerca del carácter difamatorio de unos contenidos albergados por un ISP, efectuada por la Sala Primera del Tribunal Supremo en sus sentencias de 9 de diciembre de 2009 y de 18 de mayo de 2010, y que permite tomar en consideración la comunicación efectuada por un afectado u otros datos que posibiliten su acreditación *ex re ipsa*, resulta plausible en el ámbito de aplicación de un régimen de responsabilidad civil por hecho ajeno como el previsto en el artículo 16.1 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

Dicha concreción del "conocimiento efectivo" debe quedar sujeta a límites –una tarea no llevada a cabo por el Tribunal, puesto que los casos planteados no exigían su examen-. Resulta necesario que quien ve lesionado su derecho al honor tenga la carga primaria de desplegar cierto grado de diligencia para identificar razonablemente el contenido difamatorio y su carácter ilícito, especialmente, mediante la indicación pormenorizada de URLs u otra forma de facilitar la contrastación del contenido por parte del ISP.

5. Bibliografía

David S. ARDIA (2010), "Free Speech Savior or Shield for Scoundrels: An Empirical Study of Intermediary Immunity Under Section 230 of the Communications Decency Act", 43 *Loyola of Los Angeles Law Review* 373.

Jack M. BALKIN (2009), "The Future of Free Expression in a Digital Age", 36 *Pepp. L. Rev.* 427.

José Manuel BUSTO LAGO (2008), "La responsabilidad civil de los prestadores de servicios de la sociedad de la información (ISPs)", en Luis Fernando REGLERO (Ed.), *Tratado de Responsabilidad Civil*, Tomo II, 4ª ed., Thomoson-Aranzadi, Cizur Menor.

Seth KREIMER (2006), "Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link", 155 *U. Pa. L. Rev.* 11.

Mark A. LEMLEY (2007), "Rationalizing Internet Safe Harbors", 6 *J. on Telecomm.& High Tech. L.* 101.

Ronald J. MANN y Seth R. BELZLEY (2005), "The Promise of Internet Intermediary Liability", 47 *Wm. & Mary L. Rev.* 239.

Frank PASQUALE (2007), "Copyright in an Era of Information Overload: Toward the Privileging of Categorizers", 60 *Vand. L. Rev.* 133.

Antònia PANIZA FULLANA (2010), "El alcance de la responsabilidad de los prestadores de servicios de la sociedad de la información", *Aranzadi Civil*, núm. 4, pp.27-36.

Maria Magdalena PAYERAS CAPELLÀ y Santiago CAVANILLAS MÚGICA (2005), "Los servicios de acceso y alojamiento: descripción técnica y legal", en Santiago CAVANILLAS MÚGICA, *Deberes y responsabilidades de los servidores de acceso y alojamiento. Un análisis multidisciplinar*, Comares, Granada.

Miquel PEGUERA POCH (2007), "«Sólo sé que no sé nada (efectivamente)»: la apreciación del conocimiento efectivo y otros problemas en la aplicación judicial de la LSSI", *IDP Revista d'Internet, Dret i Política* núm. 5, pp. 2-18 (disponible en http://www.uoc.edu/idp/5/dt/esp/peguera.pdf).

Miquel PEGUERA POCH (2008-2009), "The DMCA Safe Harbors and Their European Counterparts: A Comparative Analysis of Some Common Problems", 32 *Colum. J. L. & Arts* 481.

Pablo SALVADOR CODERCH et al. (2002), "Respondeat Superior I", *InDret* 2/2002 (www.indret.com)

Alan O. SYKES (1984), "The Economics of Vicarious Liability", 93 *Yale Law Journal* 1231.

Alan O. SYKES (1988), "The Boundaries of Vicarious Liability: An Economic Analysis of the Scope of Employment Rule and Related Legal Doctrines", 101 *Harvard Law Review* 563.

Jennifer M. URBAN y Laura QUILTER (2006), "Efficient Process or "Chilling Effects"? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act", 22 *Santa Clara Computer & High Tech. L.J.* 621.